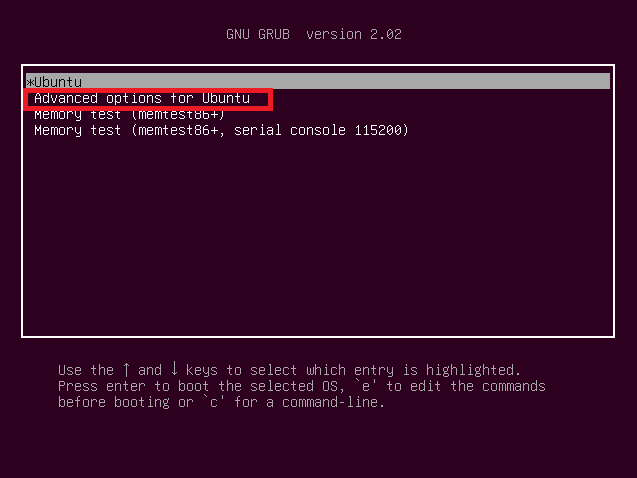
***דף מחקר פרויקט סוף - לינוקס - עידו בן זקן***

**שלב 1-**

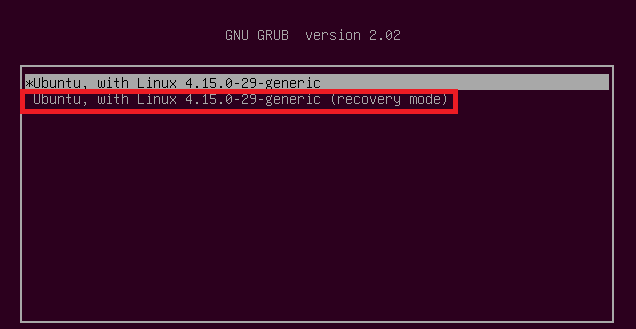
בשלב הראשון קיבלתי לידיי את המכונה הוירטואלית אותה פיתח רפי בעברו הדבר הראשון שעשיתי היה לראות עם מה יש לי לעבוד והתחלתי לבדוק דברים במכונה שהביאו לי אז התחלתי לחקור בגוגל על הגרסא של האובונטו שקיבלנו והבנתי שיש דרך להגדיר סיסמא חדשה למשתמש בגרסא זו וזה התהליך המפורט

שלב א:

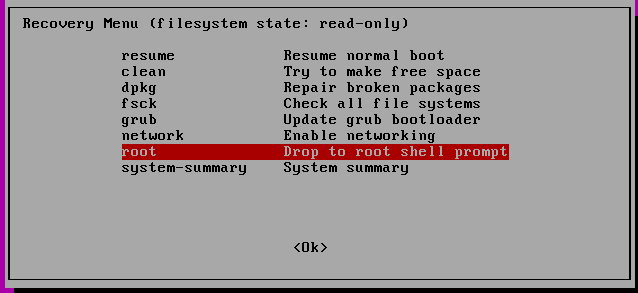
ברגע שהתוכנה עולה ניתן ללחוץ ESC וזה מה שרואים ובוחרים את האפשרות שמסומנת באדום  


שלב ב:

לאחר מכן יפתח לנו תפריט עם שתי אפשרויות לפתיחה של הגדרות האובנטו ונבחר את האופציה המסומנת באדום בתמונה הבאה



שלב ג:

לאחר שלחצנו על האופציה המסומנת באדום בשלב ב יפתח לנו התפריט הבא ואנחנו נבחר באופציה ROOT המסומנת בתמונה הבאה:

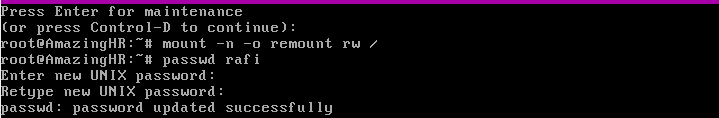
שלב ד:

לאחר שבחרנו יפתח לנו טרמינל בלמטה של המסך ואנחנו נשים את השורה הבאה בו:

mount -n -o remount rw /

לאחר מכן נכתוב:

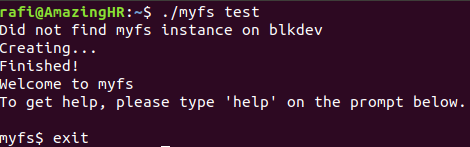
passwd <username>  
במקרה שלנו נכתוב רפי ביוזרנאיים

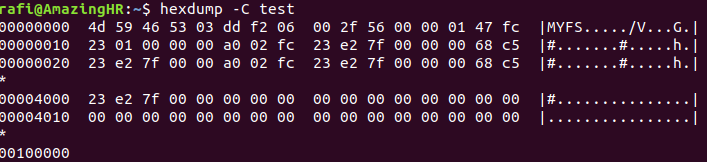
כעת תיפתח לנו אופציה חדשה שלשים סיסמא חדשה למשתמש אותו בחרנו לשנות ונבחר את הסיסמא החדשה ולאחר מכן נקליד אותה שוב כדי לאמת אותה. השיחה אמורה להיראות כך לא ניתן לראות את סיסמא ששמתי כי הם לא מראים אותה מטעמי אבטחה כנראה.

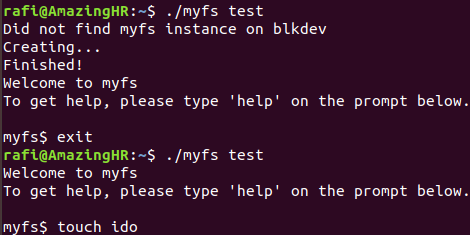
כעת הסיסמא השתנתה והצלחתי להיכנס למשתמש של רפי

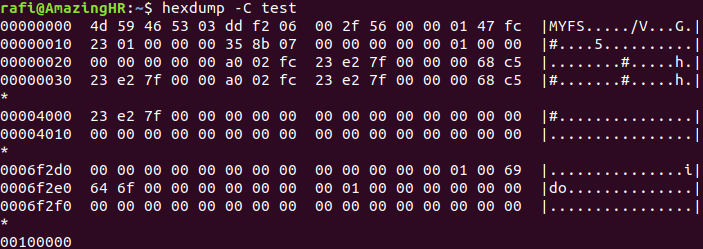
**שלב 2:**

הדבר הראשון שעשיתי היה לפתוח בHEX EDITOR את הקובץ שקיבלנו שאמור להכיל את הסיסמא שרפי החביא וראיתי שהכל כתוב כמו ערך זבל ולא ניתן למצוא כלום לאחר מכן הלכתי לגוגל וחיפשתי מידע על סוג הקובץ ועל איך ניתן להפוך אותו לקריא עבור בני אדם ורוב האתרים דיברו על הפקודה HEXDUMP בלינוקס אז חיפשתי על הפקודה וראיתי שיש לה הרבה סוגים ועברתי עליהם וראיתי שהפקודה המתאימה לי היא HEXDUMP -C היא מתרגמת את כל הקובץ בצורת טבלה של הקסאדצימלי אז ביצעתי את זה על הקובץ הנתון וקיבלתי משהו קריא שניתן להבין אבל עדיין יש הרבה בלאגן כי יש הרבה טקסטים שכתוב OLDPASS והיה גם שורה אחת בינהם שהיה כתוב את המילה PASSWORD אך זה לא הספיק לי כדי למצוא משהו אז החלטתי ליצור קובץ חדש משלי לתרגם אותו עם הפקודה ולראות איך זה נראה:

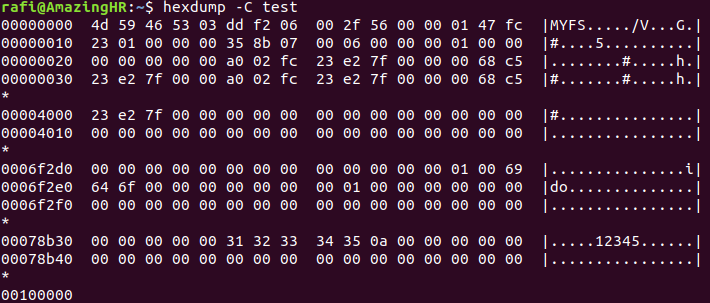
בהתחלה פתחתי קובץ בינארי בעזרת מערכת הקבצים ועוד לא הוספתי לו עוד קבצים 

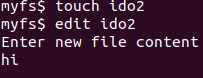
וכך זה נראה לאחר ביצוע הפקודה HEXDUMP עליו:  


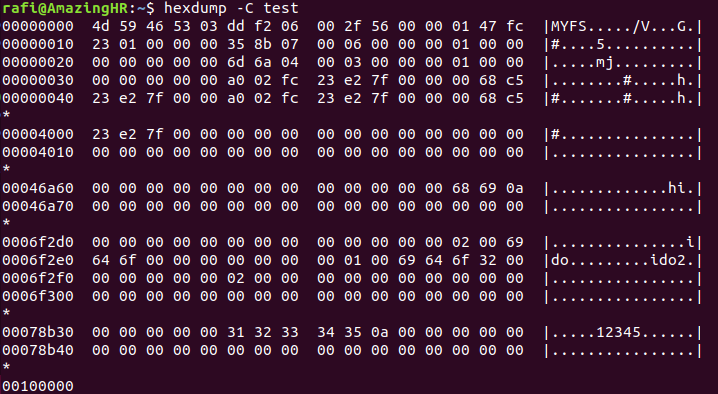
לא ממש הצלחתי להבין מזה משהו ולכן רציתי להוסיף קובץ חדש ללא תוכן עוד אז עשיתי זאת עם מערכת הקבצים  


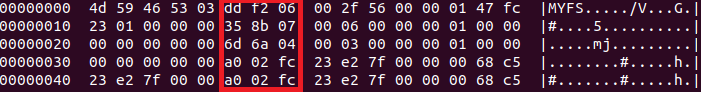
לאחר מכן הפעלתי על הקובץ עוד פעם את הפקודה HEXDUMP על הקובץ וראיתי מה השתנה

ראיתי שנוסף בלוק חדש לקובץ שמכיל את השם של הקובץ החדש שהוספתי אך זה לא נתן לי יותר מידי אז רציתי לראות מה קורה ברגע שאני מוסיף תוכן לקובץ הזה שהוספתי אז עשיתי זאת במערכת הקבצים   


ושוב בדקתי איך זה נראה בעזרת הפקודה  


כעת כבר ניתן לראות שבשורה שבה מופיע שם הקובץ מופיע הערך של השם של הקובץ בהקסאדצימלי ובנוסף יש עוד ערך מסוים שכרגע פה הוא 01 ולכן החלטתי לחקור מה הוא מייצג וכדי לעשות רציתי לראות את התנהגות הערך ברגע שאני מוסיף עוד קובץ ועורך את התוכן שלו  


וכך זה נראה:  


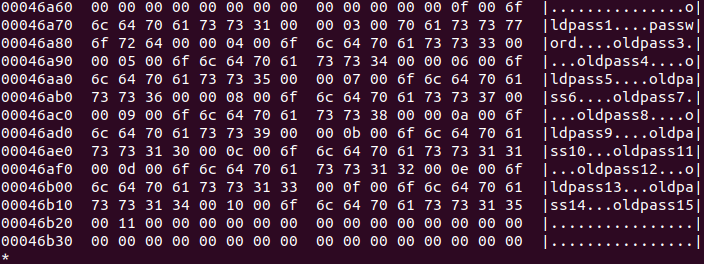
מדבר זה ניתן לראות כמה דברים הדבר הראשון הוא שהשם החדש התווסף לאותו בלוק של השם הקודם בנוסף,ניתן לראות שבשורה של שם הקובץ השני יש את הערך האקסאדצימלי של השם של הקובץ ואת הערך הנוסף שהוא 02 ולכן הבנתי שזה מונה את מספר הקבצים וזה אמור לייצג משהו בעזרת טבלת הINODES ובגלל שעל פי מה שלמדנו הטבלה נמצא בקובץ במקום ידוע מראש אז הבנתי שהיא צריכה להיות פה ממשהו שאני רואה. לאחר מכן בדקתי את הבלוק השני שניתן לראות וראיתי שהוא פשוט מכיל את הערך של # ולכן אין משהו מעניין לחפש בו ועברתי לבלוק הראשון בקובץ וראיתי שיש בו גם תאים שמייצגים את הערך שלו ויש גם תאים שלא מייצגים כלום מהאגף "המתורגם" של אותו הבלוק וראיתי שאלה שלושה תאים קבועים מבחינת מיקומם ואלה התאים הבאים:

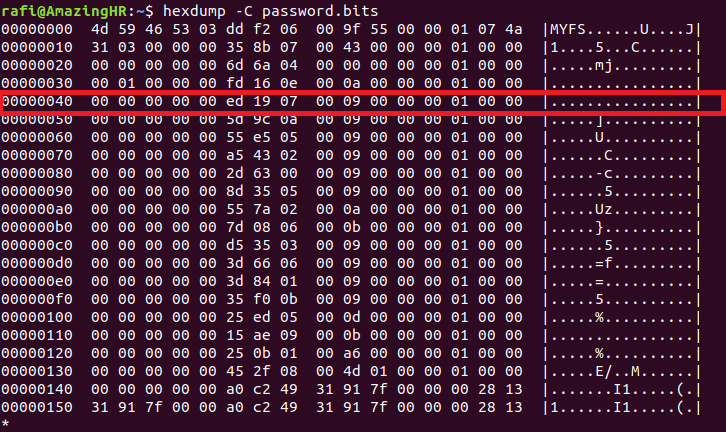
ובגלל שאני יודע שטבלת הINODES צריכה לייצג מצביע לזיכרון לתוכן של הקבצים של מערכת הקבצים אז חיפשתי קשר בין המיקום האמיתי של התוכן של הקובץ לבין התוכן של השלושה תאים האלה ושמתי לך שהתא האחרון מתוך השלושה שמסומנים מסמל את שני המספרים הראשונים של הכתובת בזיכרון של התוכן ושהתא השני מייצג את המספר השלישי והרביעי של המיקום בזיכרון של התוכן של הקובץ בזיכרון לדוגמא ניקח את התוכן של הקובץ הראשון שהוא 12345 ומיקומו 1 בטבלה על פי האינדקס שרשום בו ונראה את הקשר-

שורה בטבלת הINODES:  


מתוך מה שסימנתי פעם קודמת יוצא שהתאים שמייצגים את כתובת התוכן הם ולכן לפי מה שכתבתי נלך למקום בזיכרון שהשני מקומות הראשונים שלו הם 07 והמקום השלישי והרביעי שלו הוא 8b וזאת השורה שיוצאת לנו:  


ניתן לראות שלפי מה ששמנו בהתחלה בקובץ הראשון זה בדיוק התוכן שלו לכן הבלוק הראשון זה טבלת הINODES במערכת קבצים של רפי

לאחר שהבנו את זה נחזור לקובץ password.bits של רפי ונראה איך מה שמצאנו יכול לעזור לנו למעלה הזכרתי שראיתי את המילה password באחת מן השורות אז אני רוצה לחזור ולחקור אותה   


על פי מבנה הערכים של הבלוק הזה ניתן להבין שיש פה בהקסאדצימלי את הערך של השם שכתוב בימין ובנוסף יש לנו עוד מספר שמופיע בדיוק כמו שמות הקבצים בניסוי שאני עשיתי ולכן נילך לאיפה שרשום password כי אנחנו רוצים את הסיסמא הנוכחית ולא את הoldpass ונראה שבנוסף לערך של השם password בהקסאדצימלי יש את התא שכתוב בו 04 והבנתי שהוא יכול לייצג את האינדקס של התוכן של הקובץ בטבלת הINDOES אז עליתי הכי למעלה כי אני יודע שהבלוק הראשון הוא הטבלה והלכתי לשורה הרביעית לא כולל הראשונה כי היא 00 (השורה באדום)



כעת ניתן לראות שהתאים הרלוונטים לנו הם ולפי מה שמצאנו אנו צריכים למצוא כתובת בזיכרון שמתחילה ב 0719 לכן נלך ונחפש את הכתובת הזו בקובץ של רפי. זה מה שמצאתי  


מזה ניתן להבין שהסיסמא שאותנו אנחנו מחפשים למערכת שבנה רפי היא - **2468abcd**